

**REMARKS/ARGUMENTS**

Claims 1-48 are pending in this application. Claims 1 and 24 are independent. Claims 1-46 and 48 are amended. Claim 47 is hereby canceled without prejudice or disclaimer of its subject matter. No new matter has been added.

The courtesies extended to Applicant's representative by Examiner Sarah Su at the interview held on November 25, 2008, are appreciated. The reasons presented at the interview as warranting favorable action are incorporated into the remarks below and constitute Applicant's record of the interview

**OBJECTIONS TO THE SPECIFICATION**

In sections 4-6 on pages 2-3, the Office Action objects to the specification. In particular, the Office Action objects to the abstract, the layout of the specification, and informalities in the specification. In response, Applicant amends the abstract and specification as shown in the attached Substitute Specification. Therefore, Applicant respectfully requests withdrawal of the objections to the specification.

**OBJECTIONS TO THE CLAIMS**

In sections 7-10 on pages 3-4, the Office Action objects to claims 1-48. Applicant respectfully traverses these objections for the reasons listed below.

First, the Office Action objects to the claims because the lines of the claims are allegedly crowded too closely together. In response, all lines in the claims are now double-spaced.

Second, the Office Action alleges that claim 46 is of improper dependent form because it supposedly fails to further limit independent claim 24. In response, claim 46, by reciting a smart card, subject matter related to an apparatus, further limits the subject matter of the key generator of apparatus claim 24.

Third, the Office Action alleges that claims 14-15 are in improper form. In response, Applicant hereby replaces the reference to "any preceding claim" with -- claim 1 --.

Fourth, the Office Action objects to claim 1 because "the  $N_k$  words" allegedly lack an antecedent. In response, Applicant hereby deletes "the" before " $N_k$ " to overcome this objection.

Fifth, the Office Action objects to claim 2 because the "previously generated words" are allegedly unclear. In response, the same term in claim 1 provides an antecedent for this term in claim 2.

Sixth, the Office Action objects to claim 2 because the "subsequent words" are allegedly unclear. In response, the same term in claim 1 provides an antecedent for this term in claim 2.

Seventh, the Office Action objects to "any one of claims" in claim 11. In response, Applicant has amended claim 11 as recommended by the Examiner.

Eighth, the Office Action objects to claim 24 because “the  $N_k$  words” allegedly lack an antecedent. In response, Applicant hereby deletes “the” before “ $N_k$ ” to overcome this objection.

Ninth, the Office Action objects to claim 25 because the “previously generated words” are allegedly unclear. In response, the same term in claim 24 provides an antecedent for this term in claim 25.

Tenth, the Office Action objects to “any one of claim” in claim 34. In response, Applicant has amended claim 34 as recommended by the Examiner.

Eleventh, the Office Action objects to “any preceding” in claim 37. In response, Applicant has amended claim 37 as recommended by the Examiner.

Twelfth, the Office Action objects to claim 44. In response, Applicant has amended claim 44 as recommended by the Examiner.

Thirteenth, the Office Action objects to claim 47 because it allegedly lacks a proper transitional phrase. In response, claim 47 is canceled.

In conclusion, having addressed all of the points listed above, Applicant respectfully requests withdrawal of the objections to claims 1-48.

#### **OBJECTIONS TO THE DRAWINGS**

In sections 11-13 on pages 5-6, the Office Action objects to the drawings. Applicant respectfully traverses these objections for the reasons listed below.

First, the Office Action alleges that the drawings include particular reference characters that are not mentioned in the description. Specifically, the Office Action refers to 25 in Fig. 1, 61 in Fig. 2, 157 in Figs. 4 and 5, and 125 in Fig. 5. In response, Applicant adds a reference to 25 of Fig. 1 in paragraph [0035] of the specification, adds a reference to 63 of Fig. 2 in paragraph [0041], adds a reference to 61 of Fig. 2 in paragraph [0042], 157 of Figs. 4 and 5 in paragraph [0054], and 125 of Fig. 5 in paragraph [116]. Applicant amends the drawings to delete these reference characters.

Second, the Office Action objects to Fig. 3 due to a spelling error. The Examiner suggests changing "EXPENSION" to -- EXPANSION --. In response, Applicant amends Fig. 3 as suggested by the Examiner. Applicant also changes "OFFSETHIRD" in Fig. 3 to -- OffsetHiRd --.

Third, the Office Action alleges that Fig. 5 has not been specifically described in the specification. In response, Applicant notes that Figs. 4 and 5 are related, respectively describing encryption and decryption. As the specification describes the encryption and decryption procedures together, the same description refers to both Fig. 4 and Fig. 5. Thus, paragraph [0073] now refers to both figures.

In conclusion, having addressed all of the points listed above, Applicant respectfully requests withdrawal of the objections to the drawings.

**REJECTION UNDER 35 U.S.C. § 112, ¶2**

In sections 14-15 on page 6, the Office Action, reject claims 1 and 24 under 35 U.S.C. § 112, second paragraph as allegedly indefinite. In particular, the Office Action alleges that “the  $N_k$  words” lack a proper antecedent. Applicant respectfully traverses this rejection for the reasons listed below.

As best understood, this rejection is a duplication of the claim objections on page 4 of the Office Action. Thus, Applicant believes that deletion of “the” before “ $N_k$  words” should overcome this rejection. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 1 and 24 under 35 U.S.C. § 112, second paragraph.

**REJECTION UNDER 35 U.S.C. § 102**

In sections 16-17 on pages 6-9, the Office Action rejects claims 1-4, 6-7, 13, 20, 22-27, 29-30, 36-37, and 43-47 under 35 U.S.C. § 102(b) as allegedly anticipated by the Daemen et al article (hereinafter “Daemen”). Applicant respectfully traverses this rejection for the reasons listed below

As amended, independent claims 1 and 24 now recite, in part, “maintaining **four successive words** from the generated words in memory as long as they are required for use in the generation of subsequent words and for use in a parallel operation of a cryptographic process, wherein the four successive words comprise a **new round key**” (emphasis added). This subject matter finds support, for

example, in paragraph [0047] in the published specification. As further disclosed in paragraph [0040], each new sequence of four words, referred to as a “stretch,” comprises a new round key.

While page 15 of Daemen does indicate that round keys can be computed on-the-fly using a buffer of  $N_k$  words, Daemen does not disclose, suggest, or teach the use of four successive words. Thus, Daemen lacks subject matter now recited in claims 1 and 24. Therefore, claims 1 and 24 are allowable over Daemen.

Claims 2-4, 6-7, 13, 20, and 22-23 depend from independent claim 1. Claims 25-27, 29-30, 36-37, and 43-46 depend from independent claim 24. Thus, Applicant respectfully submits that claim 2-4, 6-7, 13, 20, 22-23, 25-27, 29-30, 36-37, and 43-46 are allowable at least on the basis of their dependencies upon allowable independent claims. Claim 47 has been canceled. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 1-4, 6-7, 13, 20, 22-27, 29-30, 36-37, and 43-47 under 35 U.S.C. § 102(b).

### **REJECTIONS UNDER 35 U.S.C. § 103**

On pages 10-14 of the Office Action, sections 18 and 19 reject claims 5, 11-12, 18-19, 21, 28, 34-35, and 41-42 under 35 U.S.C. § 103(a) as allegedly unpatentable over Daemen in view of Published U.S. Patent Application No. 2003/0223580 to Snell (hereinafter “Snell”). On pages 14-19 of the Office Action, section 20 rejects claims 8-10, 16-17, 31-33, 38-40, and 48 under 35 U.S.C. § 103(a) as allegedly

unpatentable over Daemen in view of Published U.S. Patent Application No. 2002/0191784 to Yup et al (hereinafter "Yup"). Applicant respectfully traverses this rejection for the reasons listed below

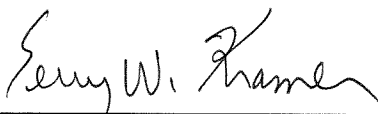
Snell and Yup fail to remedy the deficiencies of Daemen, as described above. Claims 5, 8-10, 11-12, 16-19, 21, and 48 depend from independent claim 1. Claims 28, 31-35, and 38-42 depend from independent claim 24. Thus, Applicant respectfully submits that claim 5, 8-10, 11-12, 16-19, 21, 28, 31-35, 38-42, and 48 are allowable at least on the basis of their dependencies upon allowable independent claims. Accordingly, Applicant respectfully requests withdrawal of the rejection of claims 5, 8-10, 11-12, 16-19, 21, 28, 31-35, 38-42, and 48 under 35 U.S.C. § 103(a).

**CONCLUSION**

In view of the remarks above, Applicant believes that each of the rejections/objections has been overcome and the application is in condition for allowance. In the event that the fees submitted prove to be insufficient in connection with the filing of this paper, please charge our Deposit Account Number 50-0578 and please credit any excess fees to such Deposit Account. Should there be any remaining issues that could be readily addressed over the telephone, the Examiner is asked to contact the agent overseeing the application file, Aaron Waxler, of NXP Corporation at (408) 474-5256.

Respectfully submitted,  
**KRAMER & AMADO, P.C.**

Date: December 3, 2008

  
Terry W. Kramer  
Registration No.: 41,541

Please direct all correspondence to:

Corporate Patent Counsel  
NXP Intellectual Property & Standards  
1109 McKay Drive; Mail Stop SJ41  
San Jose, CA 95131  
CUSTOMER NO.: 65913